ND-072612(J)－正誤表

IX5003/5005/5010/5020　取扱説明書

(Ver.7.8 (4.7)対応版)

正誤表

IX5003/5005/5010/5020

ネットワーク設計マニュアル編

日本電気株式会社

序

本正誤表は、IX5003/5005/5010/5020 取扱説明書（Ver. 7.8 対応 第4．7版）CD-ROM において、修正、追記された内容を記載しました。

なお、本正誤表は下記の通り各種マニュアル単位で分冊構成となっており、
本分冊の正誤表の対象マニュアルは★印で示してあります。

マニュアル内訳		正誤表
安全上のご注意	ND－072612（J）	（別冊）
IX5005／5010／5020ハードウェア取扱説明書	ND－072613（J）	（別冊）
IX5003ハードウェア取扱説明書	ND－072614（J）	（別冊）
IX5005／5010／5020工事・現調マニュアル	ND－072615（J）	（別冊）
IX5003工事・現調マニュアル	ND－072616（J）	（別冊）
IX5003／5005／5010／5020保守マニュアル	ND－072617（J）	（別冊）
IX5003／5005／5010／5020ネットワーク設計マニュアル	**ND－072618（J）**	★
IX5003／5005／5010／5020コマンドマニュアル	ND－072619（J）	（別冊）

第1．0版　2004年6月 発行　　2003年 10月31日作成以降の修正および説明追記箇所を記載

IX5003／5005／5010／5020 取扱説明書 (Ver.7.8 (4.7) 対応版)　正誤表

この度は、IX5000シリーズをご購入いただきありがとうございます。
添付の取扱説明書（CD－ROM）の記載内容に一部変更が生じましたので、以下の通り訂正いたします。
また、該当箇所の修正ページを、「添付資料」として添付致します。

1．対象マニュアル

IX5003／5005／5010／5020 ネットワーク設計マニュアル (Ver.7.8(4.7) 対応版)　ND-072618(J)

2．正誤表

項番	訂正内容	該当個所	正	備考
1	2.15 IPSec 拡張機能編 第 2 章 IPSec 拡張機能の設定	IMA-2589 《《　訂正項目 1　》》》 ●修正　：P2-1-10, 11 ●訂正詳細　：1.8.1 VR を利用した IPSec トンネル接続例 【設定例】 #ipsec address-policy IPSEC_FILTER 192.168.10.0/24 192.168.20.0/24 all allow AUTOKEY-POLICY ↓ 192.168.10.0%100/24 192.168.20.0%100/24 all allow AUTOKEY-POLICY #ipsec address-policy IPSEC_FILTER 192.168.20.0/24 192.168.10.0/24 all allow ↓ 192.168.20.0%100/24 192.168.10.0%100/24 all allow	添付資料1参照	Step7.3 以降
2	2.5 IP-QoS 拡張機能編 2.1 IP-QoS 機能の設定	DQA 対応 《《　訂正項目 1　》》》 ●修正　：P2-1-2 ●訂正詳細　：ヘッダー、フッターを下記に修正 ヘッダー（正）： IP-QoS拡張機能の設定 ND-072618(J) フッター（正）： 2-1-4 IX5003/5005/5010/5020 ネットワーク設計マニュアル-2.5 IP-QoS 拡張機能編	添付資料2参照	Step7.8 以降

項番	訂正内容	該当個所	正	備考
3	序章	《《《 訂正項目1 》》》 ●修正 ：i ●訂正詳細：下記記載を追加。 第 1.1.1 版 2004 年 02 月作成 (Software Ver.7.8.x 対応版)	添付資料3参照	Step7.8 以降
4	最終ページ	《《《 訂正項目1 》》》 ●訂正詳細：発行日の修正 2003 年 10 月 4.7 版 発行 ↓ 2004 年 2 月 4.7.1 版 発行	添付資料4参照	Step7.8 以降
5	2.15 IPSec 拡張機能編 第1章 IPSec 拡張機能概要	《《《 訂正項目 1 》》》 ●修正 ：P1-1-6,8,9 ●訂正詳細 ： 1.3 諸元 表 1-1-1 IPSec ｾｷｭﾘﾃｨｰﾎﾟﾘｼｰ数 最大 1024→2048 に変更 表 1-1-2 IKE ﾎﾟﾘｼｰ数 MAX1024→2048 に変更 1.4 制限事項 (11)・IPSec ﾄﾝﾈﾙの最大登録数の推奨値 512 以下→1024 以下 に変更 (12)・STEP7.6 から・・・→STEP7.8 から・・ に変更 ・（下記「IPSec ﾄﾝﾈﾙ数 1024 適用ﾈｯﾄﾜｰｸ構成例」を参照） →（下記「IPSec ﾄﾝﾈﾙ数 2048 適用ﾈｯﾄﾜｰｸ構成例」を参照） に変更 ・同時接続 IPSec ﾄﾝﾈﾙ数 1024→2048 に変更 ・但し 1024IPSec トンネルを収容・・・１０分程度かかります。 →但し多くの IPSec トンネルを収容・・・１０分以上かかります。 に変更 ・「IPSec ﾄﾝﾈﾙ数 1024 適用ﾈｯﾄﾜｰｸ構成例」の図 →「IPSec ﾄﾝﾈﾙ数 2048 適用ﾈｯﾄﾜｰｸ構成例」の図に変更 ・図中の IPSec Tunnel 512→1024 に変更 ・ 〃 513→1025 〃 ・ 〃 1024→2048 〃	添付資料5参照	Step7.8 以降

(注) 添付資料は該当個所に記述してあるページ数の順に添付しています。

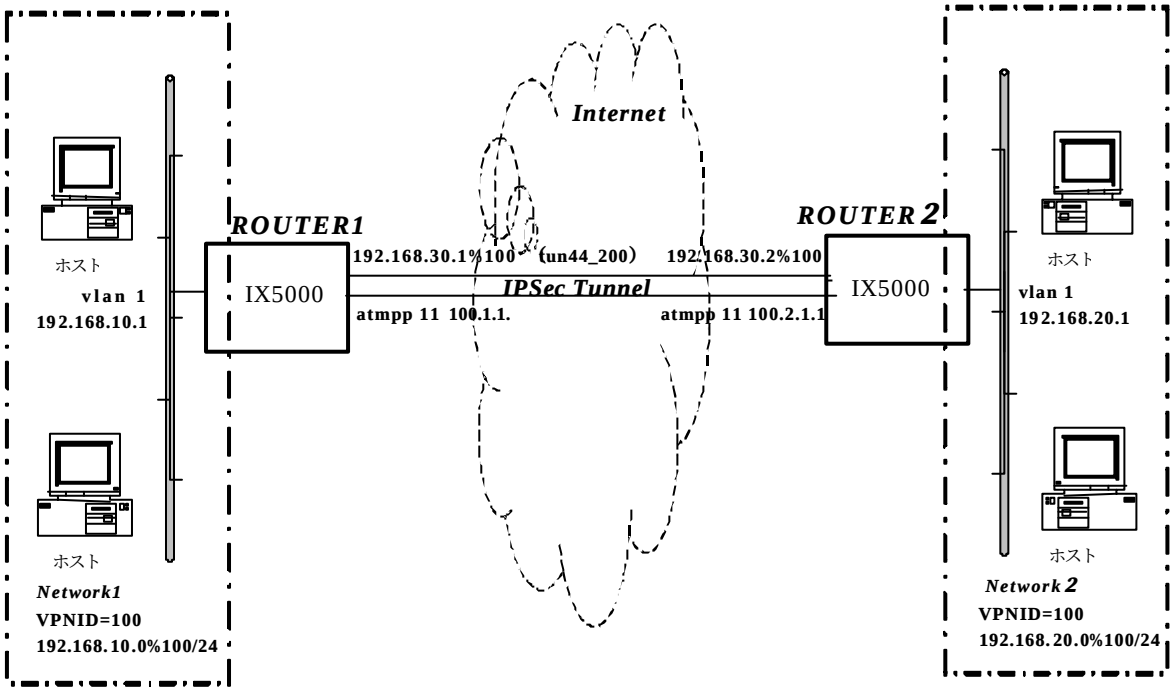
【 このページは構成の都合上空白となっています 】

添付資料1

1.8 VRを利用したIPSec設定例

1.8.1 VRを利用したIPSecトンネル接続例

【設定ネットワーク構成例】



【設定例】

[ROUTER1 の設定]

```
#ip address-table atmpp 11 100.1.1.1 255.255.255.0
#ip routing-table 100.2.1.0 255.255.255.0 100.1.1.254

#ip vrf register 100
#ip vrf interface vlan 1 100
#ip address-table vlan 1 192.168.10.1 255.255.255.0

#tunnel register tun44 200 100.1.1.1 100.2.1.1
#ip vrf interface tun44 200 100
#tunnel reachability-monitor tun44 200 disable
#tunnel ipsec tun44 200 enable
#tunnel policy-name VPNTUNNEL tun44_200 192.168.20.0%100/24 none
#ip address-table tun44 200 192.168.30.1 255.255.255.0

#ipsec autokey-proposal AUTOKEY-PROPOSAL descbc md5hmac time 3600
#ipsec autokey-policy AUTOKEY-POLICY - - - - AUTOKEY-PROPOSAL
#ipsec address-policy IPSEC_FILTER 192.168.10.0%100/24 192.168.20.0%100/24 all allow AUTOKEY-POLICY
#ipsec policy-map VPNTUNNEL IPSEC_FILTER

#ike proposal IKE_PROPOSAL - 3des sha1 modp768 time 28800
#ike policy IKE_POLICY 100.1.1.1 100.2.1.1 char ike-secret-key IKE_PROPOSAL
```

[ROUTER2 の設定]
#ip address-table atmpp 11 100.2.1.1 255.255.255.0
#ip routing-table 100.1.1.0 255.255.255.0 100.2.1.254

#ip vrf register 100
#ip vrf interface vlan 1 100
#ip address-table vlan 1 192.168.20.1 255.255.255.0

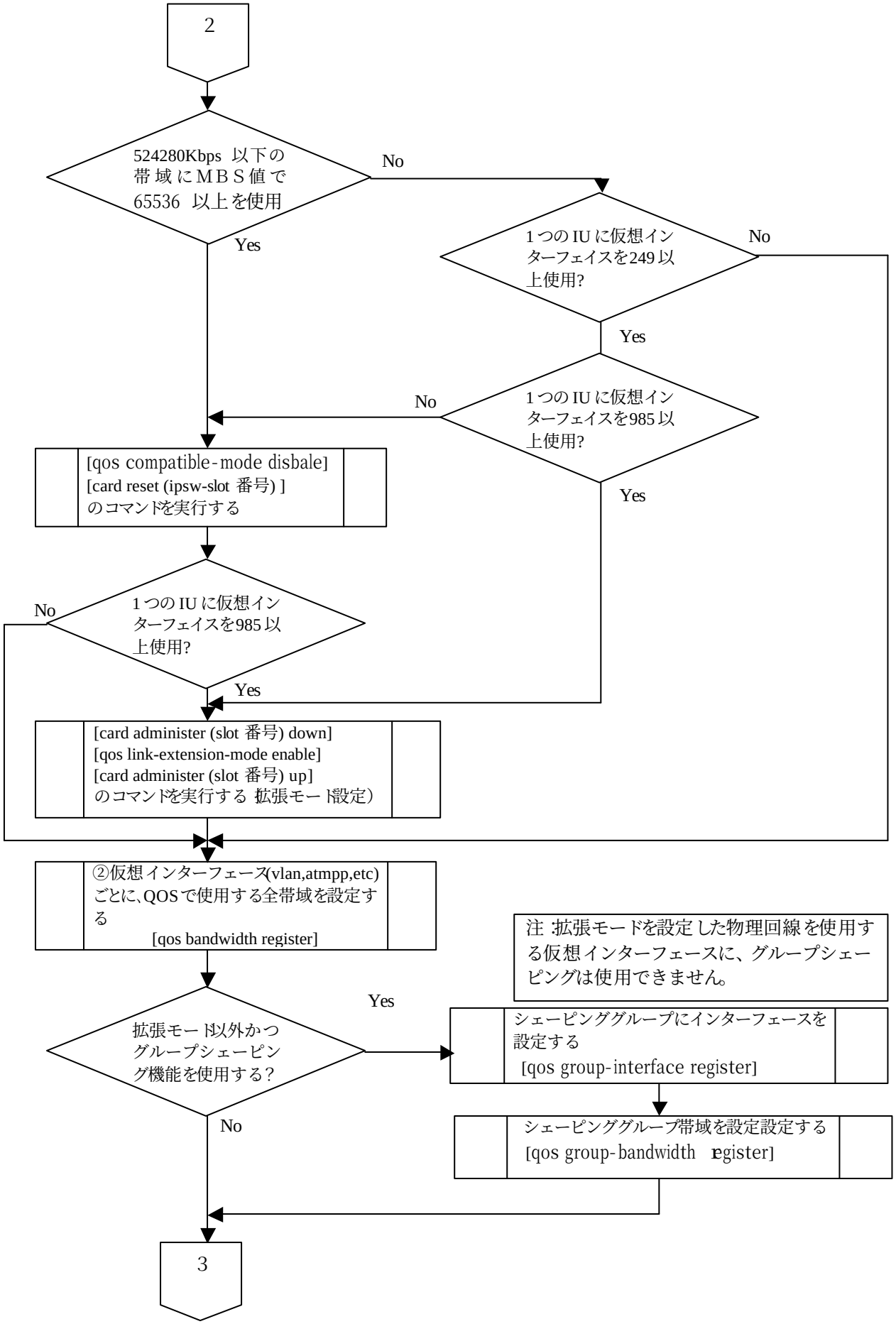
#tunnel register tun44 200 100.1.1.1 100.2.1.1
#ip vrf interface tun44 200 100
#tunnel reachability-monitor tun44 200 disable
#tunnel ipsec tun44 200 enable
#tunnel policy-name VPNTUNNEL tun44_200 192.168.10.0%100/24 none
#ip address-table tun44 200 192.168.30.2 255.255.255.0

#ipsec autokey-proposal AUTOKEY-PROPOSAL descbc md5hmac time 3600
#ipsec autokey-policy AUTOKEY-POLICY - - - - AUTOKEY-PROPOSAL
#ipsec address-policy IPSEC_FILTER 192.168.20.0%100/24 192.168.10.0%100/24 all allow
AUTOKEY-POLICY （2行にまたがっています。）
#ipsec policy-map VPNTUNNEL IPSEC_FILTER

ike proposal IKE_PROPOSAL - 3des sha1 modp768 time 28800
ike policy IKE_POLICY 100.2.1.1 100.1.1.1 char ike-secret-key IKE_PROPOSAL

※ トンネルモードの場合にはどの VPN_ID のパケットをIPSec 処理するかの設定は、ipsec address-policy コマンドで設定するのではなく、tunnel policy-name コマンドもしくはルーティングテーブル にて設定 して下さい。
本設定例は tunnel policy-name コマンドで指定した場合 について記述しています。

添付資料2


2
524280Kbps 以下の帯域にＭＢＳ値で65536 以上を使用
No
Yes
1つの IU に仮想インターフェイスを249以上使用?
No
Yes
1つの IU に仮想インターフェイスを985以上使用?
No
Yes
[qos compatible-mode disbale]
[card reset (ipsw-slot 番号)]
のコマンドを実行する
1つの IU に仮想インターフェイスを985以上使用?
No
Yes
[card administer (slot 番号) down]
[qos link-extension-mode enable]
[card administer (slot 番号) up]
のコマンドを実行する（拡張モード設定）
②仮想インターフェース(vlan,atmpp,etc)ごとに、QOSで使用する全帯域を設定する
[qos bandwidth register]
注：拡張モードを設定した物理回線を使用する仮想インターフェースに、グループシェーピングは使用できません。
拡張モード以外かつグループシェーピング機能を使用する?
Yes
No
シェーピンググループにインターフェースを設定する
[qos group-interface register]
シェーピンググループ帯域を設定設定する
[qos group-bandwidth register]
3

添付資料3

序

本説明書は IX5000シリーズネットワーク設計マニュアルについて作成しました。

第1.0版　2003年　06月作成 (Software Ver.7.6.x 対応版)
第1.1版　2003年　10月作成 (Software Ver.7.8.x 対応版)
第1.1.1版　2004年　02月作成 (Software Ver.7.8.x 対応版)

【 このページは構成の都合上空白となっています 】

添付資料4

IX5000 シリーズ　ネットワーク設計マニュアル
ND-072618(J)
2004 年 2 月　1.1.1 版　発行
発行元　日本電気株式会社 IP ネットワーク事業部
・本説明書に記載された内容は、改良のため予告なく変更することがあります。
・本製品は外国為替および外国貿易管理法により戦略物資等（または役務）に
該当しますので、日本国外に輸出する場合には、国法に基づき日本国政府の
輸出許可が必要です。
・本説明書に記載されている社名、製品名はそれぞれの会社の商標、または登録
商標です。

日本電気の許可なく複製・改変等を行うことはできません。

添付資料5

1.3 諸元

各諸元について下記表に示します。

・表 1-1-1 IPSec 機能諸元
・表 1-1-2 IKE 機能諸元
・表 1-1-3 サポートRFC
・表 1-1-4 X.509 証明書エクステンション

表 1-1-1 IPSec 機能諸元

項　　目	内　　容
IPSec モード	IPv4 over IPv4 tunnel mode IPv4 over IPv6 tunnel mode IPv6 over IPv4 tunnel mode IPv6 over IPv6 tunnel mode IPv4 transport mode IPv4 host-tunnel mode IPv6 transport mode IPv6 host-tunnel mode
サポートアルゴリズム	暗号アルゴリズム descbc/3descbc/null 認証アルゴリズム md5hmac/sha1hmac
IPSec セキュリティポリシー数	最大 2048 ・セキュリティポリシー数は ipsec address-policy コマンドの有効なコマンド設定数と一致します。セキュリティポリシー数は、下記コマンドを入力することによって全体の数が確認できます。 #show ipsec policy-map ? detail IPSec セキュリティポリシーを反映させるトンネルの最大値に関しては IPv6 拡張機能編の諸元を参照して下さい。
鍵管理方式	固定鍵（手動による鍵管理） 自動鍵（IKE による鍵管理）

表 1-1-2 IKE 機能諸元

項　　目	内　　容
実装モード	フェーズ1 メインモード/アグレッシブモード フェーズ2 クイックモード
認証方式	Pre-shared-key 方式/RSA 署名認証方式(IX5003 のみ対応)
サポートアルゴリズム	暗号アルゴリズム des/3des 認証アルゴリズム md5/sha1
サポートDH oakley group	グループ1 modp768 グループ2 modp1024
IKEポリシー数	MAX2048 ・IKE ポリシー数は ike policy コマンドで登録したポリシーエントリと ike remote-policy コマンドで登録したポリシーエントリの合計値です。
Initial-conntact 機能	・initial-contact 送信の on/off を IKE policy 毎に設定可能 ・initial-contact 送信方法(draft 準拠/nokia 対応)を IKE policy 毎に設定でき、かつ受信も両タイプについて対応可能 draft 準拠：独立した informational メッセージで送信する nokia 準拠：IKE phase1 の認証メッセージに付加して送信する 詳細については コマンドマニュアル参照
Keep-alive 機能	・keep-alive 送信の on/off を IKE policy 毎に設定可能 ・keep-alive parameter は送信間隔、無応答時の再送間隔、再送回数等の設定が可能 ・keep-alive 受信処理は常に行う ・IKE SA が収容する IPsec SA により通信が行なわれている場合は、keep-alive 送信は行なわない。(9 月末リリース時に実装) 詳細については コマンドマニュアル参照

1.4 制限事項

IX5000 シリーズにおいてIPSec 機能を使用する場合、以下の制限がありますのでご注意願います。

(1) IPSEC-ENG-A は 1 枚のみ実装可能です
将来性を考慮して複数枚実装可能となっているが現在は 1 枚しか機能しません。

(2) S/W でIPSec の処理を行う場合には、次のエンドノード動作での使用に限定してください。
- ルーティングプロトコル の認証／暗号化
- ND/RA 及びルータリナンバリング時の認証／暗号化
- ping/ping6 使用による到達確認時の認証／暗号化
- ルータの メンテナンスコネクション (telnet/telnet6 等)の認証／暗号化

(3) ユーザトラフィックへの適用は過負荷により正常動作しないことが考えられますので、IPSEC-ENG-A を実装させて H/W での IPSec 処理を行うようにして下さい。

(4) 反復トンネル (Nested Tunnel) パケットの IPSec 処理は S/W で行います。

(5) IPv4 オプション つきパケットの IPSec 処理は H/W 実装時には行えません。

(6) IPv6 拡張ヘッダつきパケットの IPSec 処理は H/W 実装時には行えません。

(7) 6K バイトを超えるパケットの IPSec 処理は行えません。

(8) 自動鍵 (IKEによる鍵管理) を使用した場合IPSec通信は通信元と通信先で相互に鍵が作成できて、初めて通信可能になります。そのため通信元と通信先で鍵作成 (鍵の初期作成 もしくは鍵の自動更新時) に時差が発生した場合は、相互に鍵が作成されるまでIPSec通信ができません。
鍵が未作成でIPSec通信ができなかった場合は、IPSec統計情報(show statistics ipsec)の下記項がカウントアップされます。
- not found esp sa もしくは not found ah sa

(9) 本装置のIPSW2重化、COM-CPU-K2重化切り替え時、切り替え前に作成した自動鍵は廃棄します。
切り替え後、下記の要求等により鍵が再作成された時点でIPSec通信の復旧が可能となります。
①本装置からの新規IPSec通信要求
②対向装置からの鍵の自動更新要求
③対向装置からのIKE Keepaliveによる鍵再作成要求

そのため対向装置からのみの片方向通信サービスで、かつ対向装置がIKE Keepalive未実装の場合は②のみが復旧手段となります。
その場合自動更新のタイミングはユーザのconfig設定であり、設定如何では復旧に時間がかかってしまう恐れがありますのでご注意ください。但し自動鍵をCLIで削除することにより回避は可能です。

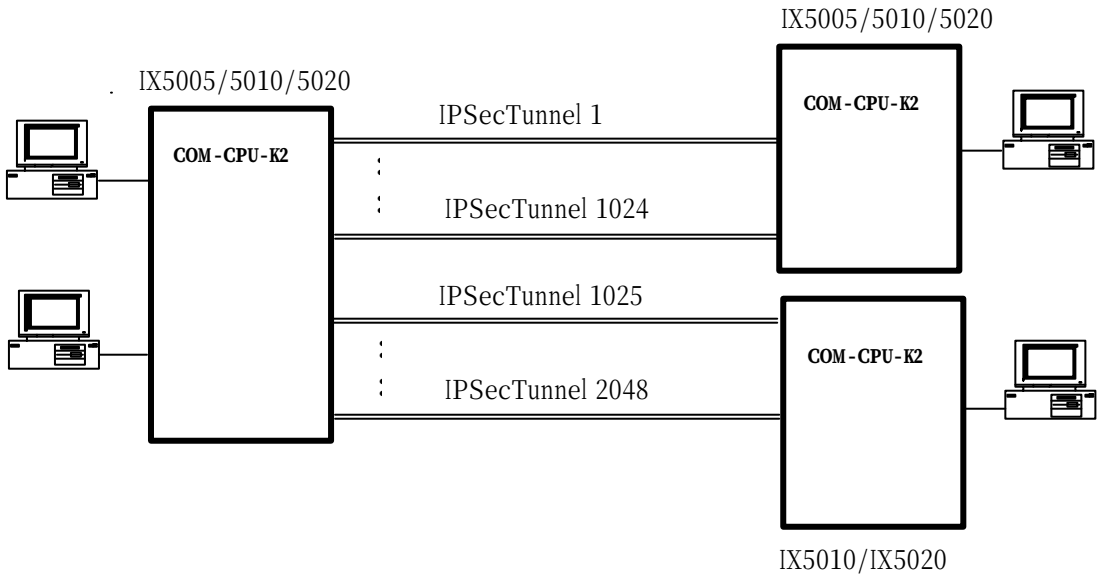
(10) ソフトウェアバージョン Ver7.4.30以前を使用している場合、同一宛先に対してIPSec有り/無しパケットが混在するようなネットワーク構成では、ハードウェア・フロー・エントリのIP-SA、L4-SP、L4-DPのマスクを解除しておく必要があります。no ipfe entry-maskコマンドにより解除設定を行って下さい。
Ver7.4.31 以降では、解除の必要はありません。

(11) トンネル番号(ID値)は2048まで登録可能ですが、IPSecトンネルの最大登録数の推奨値は、1024以下です。

(12) STEP7.8からCOM-CPU-K2使用ネットワーク (下記【IPSecトンネル数2048適用ネットワーク構成例】を参照) においてのみ同時接続IPSecトンネル数2048が可能となりましたが、運用方法に下記の制限がありますのでご注意ください。
- mainモードで、双方向から1IPSecトンネルごとに1pps程度の トラフィックの場合のみ
- Keepaliveは停止する
Defaultは、"動作する"となっているため停止してください。
Keepalive機能は、装置がrebootした場合、rebootした装置の対向装置が、reboot装置用のSAを削除し、早期復旧を目的とした機能ですが、双方向からトラフィックがある場合は、initial-contactにて同様にreboot装置用のSAを削除することができ、回避可能です。
但し多くのIPSecトンネルを収容したIX5000に障害が発生した場合、装置立ち上げ完了から全IPSec通信が復旧するまでには10分以上かかります。

・IKE eventlog/IPSec eventlogは出力しない (default:出力なし)
・SA更新時間は、1時間以上を設定する(default:1時間)

【IPSec トンネル数 2048 適用ネットワーク構成例】



(3)RSA署名認証方式に関する制限

・RSA署名認証方式はIX5003のみの対応です。

・RSA 署名認証方式を使用する場合は、cert コマンドを使用して証明書情報を事前に装置へ import する必要があります。Import した証明書情報は IPSec の RSA 署名認証に使用しますので、cert clear 等で証明書を削除した場合、削除後は RSA 署名認証での IPSec 通信ができなくなります。

添付資料 (終)